PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-096675
(43)Date of publication of application : 09.04.1999

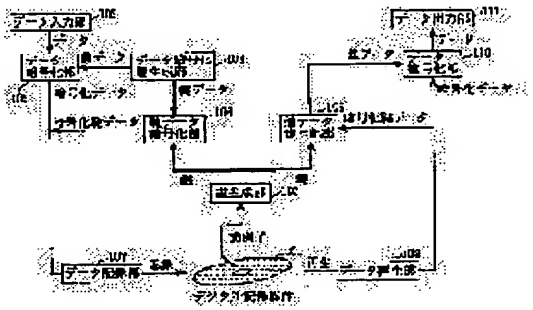
(51)Int.Cl. G11B 20/10
// G09C 1/00

(21)Application number : 09-258898
(22)Date of filing : 24.09.1997

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : YAMADA TAIJI
SUMIYOSHI TADASHI

(54) DIGITAL RECORDING MEDIUM, DATA CIPHERING DEVICE OF THE SAME, DATA DECIPHERING DEVICE, DATA CIPHERING/DECIPHERING DEVICE, ITS METHOD, AND RECORDING MEDIUM RECORDING THE METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To invalidate illegal data copying more strongly in data copying in a digital recording medium.
SOLUTION: The digital recording medium 101 records title data and an intrinsic identifier, a key generation section 102 generates a key from the identifier, a data input section 103 receives the input of the title data, a data ciphering key generation section 104 generates key data, a key data ciphering section 106 ciphers the generated key data by using the key generated by the key generation section 102, a data ciphering section 105 ciphers the title data by using the key data generated by the data ciphering key generation section 104, and a data recording section 107 records the ciphered title data and the ciphered key data in the digital recording medium 101.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－96675

(43)公開日　平成11年(1999) 4月9日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ
// Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ｄ

審査請求　未請求　請求項の数16　ＯＬ　（全 12 頁）

(21)出願番号　特願平9－258898

(22)出願日　平成９年(1997) ９月24日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　山田　泰司
愛知県名古屋市中区栄２丁目６番１号　白川ビル別館５階　株式会社松下電器情報システム名古屋研究所内

(72)発明者　住吉　正
愛知県名古屋市中区栄２丁目６番１号　白川ビル別館５階　株式会社松下電器情報システム名古屋研究所内

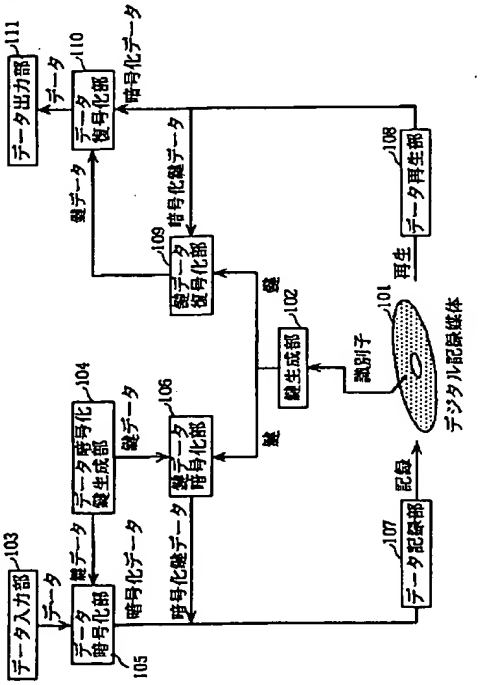
(74)代理人　弁理士　中島　司朗

(54)【発明の名称】　デジタル記録媒体、デジタル記録媒体のデータ暗号化装置、データ復号化装置、データ暗号化復号化装置、その方法及びその方法を記録した記録媒体

(57)【要約】

【課題】　デジタル記録媒体におけるデータ複製において、より強固に不正なデータ複製を無効にするデータ暗号化装置、データ復号化装置、データ暗号化復号化装置、その方法及び方法を記録した記録媒体を提供することを目的とする。

【解決手段】　デジタル記録媒体１０１はタイトルデータと固有の識別子を記録し、鍵生成部１０２は識別子から鍵を生成し、データ入力部１０３はタイトルデータの入力を受け付け、データ暗号化鍵生成部１０４は鍵データを生成し、鍵データ暗号化部１０６は生成された鍵データを鍵生成部１０２で生成された鍵を用いて暗号化し、データ暗号化部１０５はタイトルデータをデータ暗号化鍵生成部１０４で生成された鍵データを用いて暗号化し、データ記録部１０７は暗号化タイトルデータと暗号化鍵データをデジタル記録媒体１０１に記録する。



【特許請求の範囲】

【請求項１】　媒体を識別する識別子をあらかじめ記録しているデジタル記録媒体にデータを暗号化して記録するデータ暗号化装置であって、
データの入力を受け付ける入力受付手段と、
前記デジタル記録媒体より前記識別子を読み出し、読み出した識別子を基にして第１の鍵を生成する第１の鍵生成手段と、
前記入力を受け付けられたデータ毎に第２の鍵を生成する第２の鍵生成手段と、
前記入力を受け付けられたデータを前記第２の鍵を用いて暗号化し、暗号化データを生成するデータ暗号化手段と、
前記第２の鍵を前記第１の鍵を用いて暗号化し、暗号化鍵を生成する鍵暗号化手段と、
前記生成された暗号化データと前記生成された暗号化鍵とを前記デジタル記録媒体に記録する記録手段とを備えることを特徴とするデジタル記録媒体のデータ暗号化装置。

【請求項２】　前記第２の鍵生成手段は、乱数を発生させ、発生された乱数を基にして第２の鍵を生成することを特徴とする請求項１記載のデジタル記録媒体のデータ暗号化装置。

【請求項３】　前記第２の鍵生成手段は、前記入力を受け付けられたデータを基にして、第２の鍵を生成することを特徴とする請求項１記載のデジタル記録媒体のデータ暗号化装置。

【請求項４】　媒体を識別する識別子と、データを暗号化する第２の鍵を前記識別子を基にして生成された第１の鍵を用いて暗号化した暗号化鍵と、前記第２の鍵を用いて暗号化された暗号化データとをあらかじめ記録しているデジタル記録媒体よりデータを読み出して、復号化するデータ復号化装置であって、
前記デジタル記録媒体より前記識別子を読み出し、読み出した識別子を基にして第１の鍵を生成する第１の鍵生成手段と、
前記デジタル記録媒体より前記暗号化鍵と前記暗号化データとを読み出す読出手段と、
前記読み出された暗号化鍵を、前記生成された第１の鍵を基にして復号化し、第２の鍵を生成する鍵復号化手段と、
前記生成された第２の鍵を用いて、前記読み出された暗号化データを復号化するデータ復号化手段とを備えることを特徴とするデジタル記録媒体のデータ復号化装置。

【請求項５】　前記データ復号化手段は、
前記生成された第２の鍵を用いて、前記読み出された暗号化データを復号化する副復号化手段と、
前記復号化されたデータが所定の形式を形成しているかどうかを判断する形式判断手段と、
前記形式判断手段により所定の形式を形成していると判断された場合には、復号化されたデータを出力し、所定の形式を形成していないと判断された場合には、復号化されたデータの出力を抑制するデータ出力手段とを備えることを特徴とする請求項４記載のデジタル記録媒体のデータ復号化装置。

【請求項６】　媒体を識別する識別子と、データを暗号化する第２の鍵を前記識別子を基にして生成された第１の鍵を用いて暗号化した暗号化鍵と、前記第２の鍵を用いて暗号化された暗号化データとをあらかじめ記録しているデジタル記録媒体にデータを暗号化して記録し、記録されたデータを読み出して復号化するデータ暗号化復号化装置であって、
データの入力を受け付ける入力受付手段と、
前記デジタル記録媒体より前記識別子を読み出し、読み出した識別子を基にして第１の鍵を生成する第１の鍵生成手段と、
前記入力を受け付けられたデータ毎に第２の鍵を生成する第２の鍵生成手段と、
前記入力を受け付けられたデータを前記第２の鍵を用いて暗号化し、暗号化データを生成するデータ暗号化手段と、
前記第２の鍵を前記第１の鍵を用いて暗号化し、暗号化鍵を生成する鍵暗号化手段と、
前記生成された暗号化データと前記生成された暗号化鍵とを前記デジタル記録媒体に記録する記録手段と、
前記デジタル記録媒体より前記暗号化鍵と前記暗号化データとを読み出す読出手段と、
前記読み出された暗号化鍵を、前記生成された第１の鍵を基にして復号化し、第２の鍵を生成する鍵復号化手段と、
前記生成された第２の鍵を用いて、前記読み出された暗号化データを復号化するデータ復号化手段とを備えることを特徴とするデジタル記録媒体のデータ暗号化復号化装置。

【請求項７】　前記第２の鍵生成手段は、乱数を発生させ、発生された乱数を基にして第２の鍵を生成することを特徴とする請求項６記載のデジタル記録媒体のデータ暗号化復号化装置。

【請求項８】　前記第２の鍵生成手段は、前記入力を受け付けられたデータを基にして、第２の鍵を生成することを特徴とする請求項６記載のデジタル記録媒体のデータ暗号化復号化装置。

【請求項９】　前記データ復号化手段は、
前記生成された第２の鍵を用いて、前記読み出された暗号化データを復号化する副復号化手段と、
前記復号化されたデータが所定の形式を形成しているかどうかを判断する形式判断手段と、
前記形式判断手段により所定の形式を形成していると判断された場合には、復号化されたデータを出力し、所定の形式を形成していないと判断された場合には、復号化

されたデータの出力を抑制するデータ出力手段とを備えることを特徴とする請求項６記載のデジタル記録媒体のデータ暗号化復号化装置。

【請求項１０】　媒体を識別する識別子をあらかじめ記録しているデジタル記録媒体にデータを暗号化して記録するデータ暗号化方法であって、

データの入力を受け付ける入力受付ステップと、

前記デジタル記録媒体より前記識別子を読み出し、読み出した識別子を基にして第１の鍵を生成する第１の鍵生成ステップと、

前記入力を受け付けられたデータ毎に第２の鍵を生成する第２の鍵生成ステップと、

前記入力を受け付けられたデータを前記第２の鍵を用いて暗号化し、暗号化データを生成するデータ暗号化ステップと、

前記第２の鍵を前記第１の鍵を用いて暗号化し、暗号化鍵を生成する鍵暗号化ステップとを含み、

前記生成された暗号化データと前記生成された暗号化鍵とを前記デジタル記録媒体に記録することを特徴とするデジタル記録媒体のデータ暗号化方法。

【請求項１１】　前記第２の鍵生成ステップは、乱数を発生させ、発生された乱数を基にして第２の鍵を生成することを特徴とする請求項１０記載のデジタル記録媒体のデータ暗号化方法。

【請求項１２】　前記第２の鍵生成ステップは、前記入力を受け付けられたデータを基にして、第２の鍵を生成することを特徴とする請求項１０記載のデジタル記録媒体のデータ暗号化方法。

【請求項１３】　媒体を識別する識別子と、データを暗号化する第２の鍵を前記識別子を基にして生成された第１の鍵を用いて暗号化した暗号化鍵と、前記第２の鍵を用いて暗号化された暗号化データとをあらかじめ記録しているデジタル記録媒体よりデータを読み出して、復号化するデータ復号化方法であって、

前記デジタル記録媒体より前記識別子を読み出し、読み出した識別子を基にして第１の鍵を生成する第１の鍵生成ステップと、

前記デジタル記録媒体より前記暗号化鍵と前記暗号化データとを読み出す読出ステップと、

前記読み出された暗号化鍵を、前記生成された第１の鍵を基にして復号化し、第２の鍵を生成する鍵復号化ステップと、

前記生成された第２の鍵を用いて、前記読み出された暗号化データを復号化するデータ復号化ステップとを含むことを特徴とするデジタル記録媒体のデータ復号化方法。

【請求項１４】　前記データ復号化ステップは、

前記生成された第２の鍵を用いて、前記読み出された暗号化データを復号化する副復号化ステップと、

前記復号化されたデータが所定の形式を形成しているかどうかを判断する形式判断ステップと、

前記形式判断ステップにより所定の形式を形成していると判断された場合には、復号化されたデータを出力し、所定の形式を形成していないと判断された場合には、復号化されたデータの出力を抑制するデータ出力ステップとを備えることを特徴とする請求項１３記載のデジタル記録媒体のデータ復号化方法。

【請求項１５】　コンピュータ読み取り可能な記録媒体であって、

請求項１０～１４の何れかに記載の方法をコンピュータに実行させるプログラムを含むことを特徴とする記録媒体。

【請求項１６】　媒体を識別する識別子と、

データを暗号化する第２の鍵を、前記識別子を基にして生成された第１の鍵を用いて暗号化した暗号化鍵と、

前記第２の鍵を用いて暗号化された暗号化データとをあらかじめ記録していることを特徴とするデジタル記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、デジタル記録媒体、デジタル記録媒体のデータ暗号化装置、データ復号化装置、データ暗号化復号化装置、その方法及びその方法を記録した記録媒体に関する。

【０００２】

【従来の技術】近年、データのデジタル化の普及に伴い、デジタル化されたデータをデジタル記録媒体に記録し、劣化のないデータ複製が可能となった。一方、データを提供する側の著作権を保護する立場から、データのデジタル記録媒体への記録に関して、データ複製管理装置としてデジタルオーディオテープ（ＤＡＴ）カセットシステム（日本電子機械工業会技術レポートＥＩＡＪ ＣＰＲ-２３０４　DAT Cassette System　Part6：Serial Copy Management System）や、光ディスクの不正コピー防止装置として、光記録媒体の再生装置（特開平７-２１６８７、特開平7-２１６８８、特開平7-８５５７４）が提案されている。

【０００３】図４は、前記ＤＡＴカセットシステムにおけるデータ複製管理装置の構成図である。図４のデータ複製管理装置は、デジタルオーディオなどを入力するデータ入力部２１、デジタル記録媒体へのデータ記録時に入力データ中の複製制御情報を判断する複製制御情報管理部２２、複製制御情報管理部２２での判断に従ってデータを記録するデジタル記録媒体２３、デジタル記録媒体から読み込んだデータを出力するデータ出力部２４から構成される。次に、図４のデータ複製管理装置の動作を説明する。デジタル記録媒体２３へデータを記録する場合に、複製制御情報管理部２２は、データ入力部２１から入力されたデータ中の複製可能かどうかを示す複製制御情報を基に判断し、複製可能であると判断したとき

は、以降の複製が可能かどうかを示す制御情報を複製不可能に設定して、データと併せて前記制御情報を暗号化せずに平文でデジタル記録媒体２３に記録する。入力データ中の複製制御情報が複製不可能であると判断したときは、デジタル記録媒体２３へ記録は行なわない。デジタル記録媒体２３からのデータの再生時には、データ出力部２４は、デジタル記録媒体２３から読み込んだデータを出力する。このようにして、図４のデータ複製管理装置では、データの無制限の複製を抑制している。

【０００４】図５、図６は、特開平7-２１６８７、特開平7-２１６８８、特開平7-８５５７４に開示された光ディスクの不正コピー防止装置の構成図である。図５は、光ディスクの不正コピー防止装置の記録部の構成図であり、光ディスク３１、原データをキー情報で暗号化し主データを出力する暗号化手段３３、出力された主データを光ディスクに対して記録する主データ記録手段３４、入力されたキー情報を光ディスクのデータ記録領域以外の領域に記録するキー情報記録手段３５から構成される。

【０００５】図６は、光ディスクの不正コピー防止装置の再生部の構成図であり、光ディスク４１、光ディスク４１からの主データを読み込む主データ読取手段４３、光ディスク４１からのキー情報を読み込むキー情報読取手段４４、主データ読取手段４３から出力される主データを、キー情報読取手段４４から出力されるキー情報によって復号化して原データを出力する復号化手段４５から構成される。

【０００６】ここで、データ記録領域以外の領域とは、光ディスクの外周側端部、光ディスクのデータ記録部とは反対面に形成されたレーベル記録面などを言う。図５、図６に示す光ディスクの不正コピー防止装置の動作を以下に説明する。データを記録する場合には、暗号化手段３３は、入力されたキー情報によって原データを暗号化して主データとして主データ記録手段３４へ出力する。主データ記録手段３４は、出力された主データを光ディスク３１に記録し、キー情報記録手段３５は、暗号化に用いたキー情報を光ディスク３１に記録する。この時、キー情報は光ディスクのデータ記録領域以外の領域に記録される。データを読み込む場合には、主データ読取手段４３は、光ディスク４１から主データを読み込み、キー情報読取手段４４は、光ディスク４１のデータ記録領域以外の領域からキー情報を読み込む。復号化手段４５は、キー情報を用いて主データを復号化して原データを出力する。このようにして、図５、図６に示す光ディスクの不正コピー防止装置では、データ記録領域以外の領域にキー情報を書き込むことにより、光記録媒体のコストアップを最小限に抑えながら、不正コピーを防止することができる。

【０００７】

【発明が解決しようとする課題】従来のデータ複製管理装置としてのＤＡＴカセットシステムでは、データの無制限の複製を抑制しているものの、デジタルデータが複製可能かどうかを示す複製制御情報が平文でデジタル記録媒体に記録されている為、複製制御情報の改竄による不正複製が比較的容易にできるという問題点があり、またデジタル記録媒体に記録されているデータと複製制御情報をそのまま別のデジタル記録媒体に複製することによる不正複製も比較的容易にできるという問題点がある。

【０００８】また、「特開平７－８５５７４」、「特開平７－２１６８７」、「特開平７－21６８８」で開示されている不正コピー防止装置では、光記録媒体のコストアップを最小限に抑えながら、不正コピーを防止しているものの、暗号化に用いたキー情報が平文でディスクのデータ領域以外の領域に記録されている為、キー情報を読み込めば、不正にデータの復号化が可能であるという問題点があり、また、ディスク上の全記録データに対してキー情報が共通である為、キー情報が不正に入手されれば、その結果、ディスク上のすべての記録データを不正に復号化できるという問題点がある。

【０００９】本発明は、前記の問題点に鑑み、デジタル記録媒体におけるデータ複製において、より強固に不正なデータ複製を無効にするデータ暗号化装置、データ復号化装置、データ暗号化復号化装置、その方法及びその方法を記録した記録媒体を提供することを目的とするものである。

【００１０】

【課題を解決するための手段】前記の目的を達成するために、本発明は、媒体を識別する識別子をあらかじめ記録しているデジタル記録媒体にデータを暗号化して記録するデータ暗号化装置であって、データの入力を受け付ける入力受付手段と、前記デジタル記録媒体より前記識別子を読み出し、読み出した識別子を基にして第１の鍵を生成する第１の鍵生成手段と、前記入力を受け付けられたデータ毎に第２の鍵を生成する第２の鍵生成手段と、前記入力を受け付けられたデータを前記第２の鍵を用いて暗号化し、暗号化データを生成するデータ暗号化手段と、前記第２の鍵を前記第１の鍵を用いて暗号化し、暗号化鍵を生成する鍵暗号化手段と、前記生成された暗号化データと前記生成された暗号化鍵とを前記デジタル記録媒体に記録する記録手段とを備えることを特徴とする。

【００１１】ここで、前記第２の鍵生成手段は、乱数を発生させ、発生された乱数を基にして第２の鍵を生成するように構成してもよい。ここで、前記第２の鍵生成手段は、前記入力を受け付けられたデータを基にして、第２の鍵を生成するように構成してもよい。また、本発明は、媒体を識別する識別子と、データを暗号化する第２の鍵を前記識別子を基にして生成された第１の鍵を用いて暗号化した暗号化鍵と、前記第２の鍵を用いて暗号化

された暗号化データとをあらかじめ記録しているデジタル記録媒体よりデータを読み出して、復号化するデータ復号化装置であって、前記デジタル記録媒体より前記識別子を読み出し、読み出した識別子を基にして第１の鍵を生成する第１の鍵生成手段と、前記デジタル記録媒体より前記暗号化鍵と前記暗号化データとを読み出す読出手段と、前記読み出された暗号化鍵を、前記生成された第１の鍵を基にして復号化し、第２の鍵を生成する鍵復号化手段と、前記生成された第２の鍵を用いて、前記読み出された暗号化データを復号化するデータ復号化手段とを備えることを特徴とする。

【００１２】ここで、前記データ復号化手段は、前記生成された第２の鍵を用いて、前記読み出された暗号化データを復号化する副復号化手段と、前記復号化されたデータが所定の形式を形成しているかどうかを判断する形式判断手段と、前記形式判断手段により所定の形式を形成していると判断された場合には、復号化されたデータを出力し、所定の形式を形成していないと判断された場合には、復号化されたデータの出力を抑制するデータ出力手段とを備えるように構成してもよい。

【００１３】また、本発明は、媒体を識別する識別子と、データを暗号化する第２の鍵を前記識別子を基にして生成された第１の鍵を用いて暗号化した暗号化鍵と、前記第２の鍵を用いて暗号化された暗号化データとをあらかじめ記録しているデジタル記録媒体にデータを暗号化して記録し、記録されたデータを読み出して復号化するデータ暗号化復号化装置であって、データの入力を受け付ける入力受付手段と、前記デジタル記録媒体より前記識別子を読み出し、読み出した識別子を基にして第１の鍵を生成する第１の鍵生成手段と、前記入力を受け付けられたデータ毎に第２の鍵を生成する第２の鍵生成手段と、前記入力を受け付けられたデータを前記第２の鍵を用いて暗号化し、暗号化データを生成するデータ暗号化手段と、前記第２の鍵を前記第１の鍵を用いて暗号化し、暗号化鍵を生成する鍵暗号化手段と、前記生成された暗号化データと前記生成された暗号化鍵とを前記デジタル記録媒体に記録する記録手段と、前記デジタル記録媒体より前記暗号化鍵と前記暗号化データとを読み出す読出手段と、前記読み出された暗号化鍵を、前記生成された第１の鍵を基にして復号化し、第２の鍵を生成する鍵復号化手段と、前記生成された第２の鍵を用いて、前記読み出された暗号化データを復号化するデータ復号化手段とを備えることを特徴とする。

【００１４】ここで、前記第２の鍵生成手段は、乱数を発生させ、発生された乱数を基にして第２の鍵を生成するように構成してもよい。ここで、前記第２の鍵生成手段は、前記入力を受け付けられたデータを基にして、第２の鍵を生成するように構成してもよい。ここで、前記データ復号化手段は、前記生成された第２の鍵を用いて、前記読み出された暗号化データを復号化する副復号化手段と、前記復号化されたデータが所定の形式を形成しているかどうかを判断する形式判断手段と、前記形式判断手段により所定の形式を形成していると判断された場合には、復号化されたデータを出力し、所定の形式を形成していないと判断された場合には、復号化されたデータの出力を抑制するデータ出力手段とを備えるように構成してもよい。

【００１５】また、本発明は、媒体を識別する識別子をあらかじめ記録しているデジタル記録媒体にデータを暗号化して記録するデータ暗号化方法であって、データの入力を受け付ける入力受付ステップと、前記デジタル記録媒体より前記識別子を読み出し、読み出した識別子を基にして第１の鍵を生成する第１の鍵生成ステップと、前記入力を受け付けられたデータ毎に第２の鍵を生成する第２の鍵生成ステップと、前記入力を受け付けられたデータを前記第２の鍵を用いて暗号化し、暗号化データを生成するデータ暗号化ステップと、前記第２の鍵を前記第１の鍵を用いて暗号化し、暗号化鍵を生成する鍵暗号化ステップとを含み、前記生成された暗号化データと前記生成された暗号化鍵とを前記デジタル記録媒体に記録することを特徴とする。

【００１６】ここで、前記第２の鍵生成ステップは、乱数を発生させ、発生された乱数を基にして第２の鍵を生成するように構成してもよい。ここで、前記第２の鍵生成ステップは、前記入力を受け付けられたデータを基にして、第２の鍵を生成するように構成してもよい。また、本発明は、媒体を識別する識別子と、データを暗号化する第２の鍵を前記識別子を基にして生成された第１の鍵を用いて暗号化した暗号化鍵と、前記第２の鍵を用いて暗号化された暗号化データとをあらかじめ記録しているデジタル記録媒体よりデータを読み出して、復号化するデータ復号化方法であって、前記デジタル記録媒体より前記識別子を読み出し、読み出した識別子を基にして第１の鍵を生成する第１の鍵生成ステップと、前記デジタル記録媒体より前記暗号化鍵と前記暗号化データとを読み出す読出ステップと、前記読み出された暗号化鍵を、前記生成された第１の鍵を基にして復号化し、第２の鍵を生成する鍵復号化ステップと、前記生成された第２の鍵を用いて、前記読み出された暗号化データを復号化するデータ復号化ステップとを含むことを特徴とする。

【００１７】ここで、前記データ復号化ステップは、前記生成された第２の鍵を用いて、前記読み出された暗号化データを復号化する副復号化ステップと、前記復号化されたデータが所定の形式を形成しているかどうかを判断する形式判断ステップと、前記形式判断ステップにより所定の形式を形成していると判断された場合には、復号化されたデータを出力し、所定の形式を形成していないと判断された場合には、復号化されたデータの出力を抑制するデータ出力ステップとを備えるように構成して

もよい。

【００１８】また、本発明は、コンピュータ読み取り可能な記録媒体であって、上記の方法をコンピュータに実行させるプログラムを含むことを特徴とする。また、本発明は、デジタル記録媒体であって、媒体を識別する識別子と、データを暗号化する第２の鍵を前記識別子を基にして生成された第１の鍵を用いて暗号化した暗号化鍵と、前記第２の鍵を用いて暗号化された暗号化データとをあらかじめ記録していることを特徴とする。

【００１９】

【発明の実施の形態】次に、本発明に係る一つの実施の形態としてのデータ暗号化復号化装置について説明する。

（データ暗号化復号化装置の構成）ここでは、本発明の一つの実施の形態としてのデータ暗号化復号化装置の構成を図１に示すブロック図を用いて説明する。

【００２０】図１のデータ暗号化復号化装置は、デジタル記録媒体１０１、鍵生成部１０２、データ入力部１０３、データ暗号化部１０５、データ暗号化鍵生成部１０４、鍵データ暗号化部１０６、データ記録部１０７、データ出力部１１１、データ復号化部１１０、鍵データ復号化部１０９、データ再生部１０８から構成される。デジタル記録媒体１０１は、Ｄｉｇｉｔａｌ　Ｖｉｄｅｏ　Ｄｉｓｃ（以下、ＤＶＤと略す。）－Ｒａｍｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙなどからなり、動画などのタイトルデータと、予め消去不可能な領域に媒体毎に異なり固有に割り付けられた識別子とを記録している。

【００２１】鍵生成部１０２は、デジタル記録媒体１０１から媒体固有の識別子を読み込み、読み込んだ識別子を元に鍵を生成する。鍵の生成方法としては、例えば、前記読み出した識別子の内の複数の特定のバイトを取りだして、そのバイトを鍵とする方法や、前記取り出したバイトに対して所定のビット演算を施すなどの方法がある。

【００２２】データ入力部１０３は、タイトルデータをデジタル記録媒体１０１に記録する場合にタイトルデータの入力を受け付け、入力を受け付けられたデータをデータ暗号化部１０５に出力する。また、データ入力部１０３は、タイトルデータの入力が終了したかどうかを判断し、入力が終了するまで、データの入力の受付けを繰り返す。

【００２３】データ暗号化鍵生成部１０４は、鍵データを生成し、鍵データ暗号化部１０６及びデータ暗号化部１０５に出力する。鍵データの生成方法として、乱数を発生させ、その乱数の内の複数の特定のバイトを取りだして、そのバイトを鍵とする方法、前記取り出した特定のバイトに対して所定のビット演算を施す方法、また、データ入力部１０３により、入力を受け付けられたタイトルデータを元に鍵データを生成する方法、データ入力部１０３からタイトルデータと共にタイトルデータを識別するタイトルコードの入力を受け付け、入力を受け付けられたタイトルコードを元に鍵データを生成する方法がある。この場合には、データ入力部１０３は、データ暗号化鍵生成部１０４にタイトルデータ又はタイトルコードを出力する。

【００２４】鍵データ暗号化部１０６は、データ暗号化鍵生成部１０４で生成された鍵データを、鍵生成部１０２で生成された鍵を用いて暗号化し、データ記録部１０７に出力する。次に、この場合に用いる暗号化の一例を示す。鍵生成部１０２で生成された鍵の値が、例えば、「３５４８６９」であった場合、データ暗号化鍵生成部１０４で生成された鍵データに対して、鍵の値の最初の１桁が「３」であるので、前記鍵データの先頭から３バイト毎にビット反転グループとし、鍵の値の２桁目の「５」が奇数であるので、先頭からの奇数番目の前記ビット反転グループをビット反転する。次に、鍵の値の３桁目が「４」であるので、前記鍵データの先頭から４ビット毎に左シフトグループとし、鍵の値の４桁目が「８」であるので、前記左シフトグループ毎に、８ビットだけ左へラウンドシフトする。さらに、鍵の値の５桁目が「６」であるので、前記鍵データの先頭から６ビット毎に右シフトグループとし、鍵の値の６桁目が「９」であるので、前記右シフトグループ毎に、９ビットだけ右へラウンドシフトする。ここで、ビット列を左へラウンドシフトするとは、指定されたビット数だけビット列を左へシフトし、左へシフトした場合にビット列からあふれ出たビットを、ビット列の右側に付加する動作をいうこととする。また、右へのラウンドシフトについても同様とする。

【００２５】データ暗号化部１０５は、データ入力部１０３から入力されたタイトルデータを、データ暗号化鍵生成部１０４で生成された鍵データを用いて暗号化し、暗号化されたタイトルデータをデータ記録部１０７に出力する。この暗号化方法については、鍵データ暗号化部１０６で一例を示した暗号化方法と同一の方法としてもよい。ここでは、また別の一例を次に示す。例えば、データ暗号化鍵生成部１０４で生成された鍵データの値が「５９２４１」であった場合、データ入力部１０３が入力を受け付けたデータに対して、前記鍵データの値の最初の１桁が「５」であるので、前記データの先頭から５バイト毎にビット反転グループとし、前記鍵データの値の２桁目の「９」が奇数であるので、前記ビット反転グループ内の先頭からの奇数番目のバイトをビット反転する。次に、前記データの先頭から前記鍵データの値の３桁目の「２」バイト毎にシフトグループとし、前記シフトグループ毎に、鍵データの値の４桁目の「４」が偶数なので左へ、前記鍵データの値の５桁目の「１」で示されたビット数だけラウンドシフトする。

【００２６】データ記録部１０７は、データ暗号化部１０５で暗号化されたタイトルデータと鍵データ暗号化部

１０６で暗号化された鍵データとをデジタル記録媒体１０１に記録する。暗号化鍵データと暗号化データの記録方法については、暗号化鍵データをまず書き込み、その次に暗号化データを書き込むとすることができる。また、暗号化データをあらかじめ決めておいたバイトに分割し、分割されたバイトの間隔に、暗号化鍵データを分割して記録するとしてもよい。これにより、さらにタイトルデータの保守性が高められるのは明らかである。

【００２７】データ再生部１０８は、デジタル記録媒体１０１から暗号化鍵データと暗号化データとを読み込み、読み込んだ暗号化データと、暗号化鍵データを分離し、暗号化鍵データを鍵データ復号化部１０９に出力し、暗号化データをデータ復号化部１１０に出力する。また、データ再生部１０８は、暗号化データの読込みが終了したかどうかを判断し、暗号化データの読込みが終了していなければ、終了するまで読込みを繰り返す。

【００２８】鍵データ復号化部１０９は、鍵生成部１０２から生成された鍵により復号化方式を決定する。ここで復号化の方式としては、データ記録時の鍵データ暗号化部１０６で採用した暗号化方法の逆の手順を採用する。また、鍵データ復号化部１０９は、鍵生成部１０２から生成された鍵を用いて、データ再生部１０８から出力された暗号化鍵データを復号化し、データ復号化部１１０に出力する。

【００２９】データ復号化部１１０は、データ再生部１０８から出力された暗号化データを、鍵データ復号化部１０９で復号化された鍵データを用いて、復号化し、タイトルデータとしてデータ出力部１１１に出力する。復号化の方法としてはデータ記録時のデータ暗号化部１０５で採用した暗号化方法の逆の手順を採用する。

（データ暗号化復号化装置のデータ記録動作）ここでは、図１に示すデータ暗号化復号化装置のタイトルデータの記録動作について、図２のフローチャートを用いて説明する。

【００３０】デジタル記録媒体がＤＶＤレコーダなどのデータ暗号化復号化装置にセットされると、鍵生成部１０２は、デジタル記録媒体から識別子を読み込み、その識別子を元に暗号化の為の鍵を生成し（ステップＦ５１）、鍵データ暗号化部１０６は、鍵生成部１０２で生成された鍵により暗号化方法を決定し（ステップＦ５２）、データ暗号化鍵生成部１０４は、鍵データを生成し（ステップＦ５３）、データ暗号化部１０５は、データ暗号化鍵生成部１０４で生成された鍵データにより暗号化方法を決定する（ステップＦ５４）。データ入力部１０３は、タイトルデータの入力が終了したかどうかを判断し、入力が終了したと判断した場合は（ステップＦ５５）、処理を終了し、入力が終了していないと判断した場合は（ステップＦ５５）、データ入力部１０３は、タイトルデータの入力を受け付け（ステップＦ５６）、鍵データ暗号化部１０６は、ステップＦ５２で決定した暗号化方法に従って、鍵データを暗号化してデータ記録部１０７に出力し（ステップＦ５７）、データ暗号化部１０５は、ステップＦ５４で決定した暗号化方法に従って、データ入力部１０３が受け付けたタイトルデータを暗号化して、データ記録部１０７に出力し（ステップＦ５８）、データ記録部１０７は、前記暗号化された鍵データと、暗号化されたタイトルデータをデジタル記録媒体１０１に記録し（ステップＦ５９）、再度ステップＦ５５に戻る。ステップＦ５６からステップＦ５９の処理をタイトルデータが入力されている間繰り返し、タイトルデータの入力が完了した時点で書込み処理が終了する。

（データ複製管理装置のデータ再生動作）ここでは、図１に示すデータ暗号化復号化装置のタイトルデータの再生動作について図３のフローチャートを用いて説明する。

【００３１】ＤＶＤレコーダなどのデータ暗号化復号化管理にデジタル記録媒体がセットされると、鍵生成部１０２は、デジタル記録媒体から識別子を読み込み、その識別子を元に復号化の為の鍵を生成し（ステップＦ６１）、鍵データ復号化部１０９は、鍵生成部１０２で生成された鍵により復号化方式を決定し（ステップＦ６２）、データ再生部１０８は、デジタル記録媒体１０１から、暗号化鍵データを読み込み、暗号化鍵データを鍵データ復号化部１０９に出力し（ステップＦ６３）、鍵データ復号化部１０９は、ステップＦ６１で決定された復号化方式に従って、読み込まれた暗号化鍵データを復号化し（ステップＦ６４）、データ復号化部１１０は、鍵データ復号化部１０９において復号化された鍵データにより復号化方法を決定する（ステップＦ６５）。データ再生部１０８は、デジタル記録媒体１０１から暗号化データを読み込み（ステップＦ６６）、データ再生部１０８は、暗号化データの読込みが終了したかどうかを判断し、読込みが終了したと判断した場合は（ステップＦ６７）、処理を終了し、読込みが終了していないと判断した場合は（ステップＦ６７）、データ復号化部１１０は、デジタル記録媒体１０１からデータ再生部１０８により読み込まれた暗号化データを、鍵データ復号化部１０９により復号化された鍵データを用いて復号化し（ステップＦ６８）、データ出力部１１１は、復号化された暗号化データを出力する（ステップＦ６９）。データ再生部１０８からの暗号化データの読込みが完了するまでステップＦ６６からステップＦ６９の処理を繰り返し、デジタル記録媒体からの暗号化されたデータの読込みが完了した時点でタイトルデータの再生動作を終了する。

【００３２】以上説明した構成によると、暗号化データと暗号化鍵データとが不正に複製されたデジタル媒体を再生する場合、当該デジタル媒体の識別子から生成された鍵と、前記暗号化鍵データを暗号化した鍵とが一致しないので、暗号化鍵データは正しい鍵データに復号化さ

れない。次に、正しく復号化されなかった鍵データを用いて、暗号化データを復号しても、正しいデータに復号されない。このように、デジタル記録媒体を不正に複製した場合には、正しいデータが再生できない。ということが分かる。

【００３３】なお、デジタル記録媒体に記録されたデータがＭＰＥＧなどの規格化されたデータである場合には、データ復号化部１１０は、復号したデータが、ＭＰＥＧなどの規格化されたデータ形式に適合しているかどうかをチェックして、適合しないデータ形式であった場合には、当該データは不正に複製されたものとみなし、データ再生部１０８に対してデジタル記録媒体からのデータ読込みを中止し、適合したデータ形式であった場合には、デジタル記録媒体からのデータ読込みを継続する構成とすることもできる。

【００３４】

【発明の効果】以上説明したように、本発明は、媒体を識別する識別子をあらかじめ記録しているデジタル記録媒体にデータを暗号化して記録するデータ暗号化装置であって、データの入力を受け付ける入力受付手段と、前記デジタル記録媒体より前記識別子を読み出し、読み出した識別子を基にして第１の鍵を生成する第１の鍵生成手段と、前記入力を受け付けられたデータ毎に第２の鍵を生成する第２の鍵生成手段と、前記入力を受け付けられたデータを前記第２の鍵を用いて暗号化し、暗号化データを生成するデータ暗号化手段と、前記第２の鍵を前記第１の鍵を用いて暗号化し、暗号化鍵を生成する鍵暗号化手段と、前記生成された暗号化データと前記生成された暗号化鍵とを前記デジタル記録媒体に記録する記録手段とを備える。

【００３５】この構成によると、デジタル記録媒体毎に異なり固有に割り付けられた識別子から生成した鍵を用いて、タイトルデータを暗号化したその鍵データ自身を暗号化するので、暗号化タイトルデータを復号する際の鍵データ自身の保護強度を高めるという効果がある。また、タイトルデータ毎に異なった鍵データによって暗号化が行なわれる為、あるタイトルデータの暗号化に使用された鍵データが不正に入手されても、デジタル記録媒体上の他のタイトルデータに対する不正なアクセスからは保護されるという効果があり、その結果としてデジタル記録媒体の不正な複製や、タイトルデータの鍵データ不正入手に対しても高いセキュリティの実現が可能となる。

【００３６】ここで、前記第２の鍵生成手段は、乱数を発生させ、発生された乱数を基にして第２の鍵を生成するように構成してもよい。この構成によると、鍵データが乱数を基に生成されるので、鍵データを発見されにくくするという効果がある。ここで、前記第２の鍵生成手段は、前記入力を受け付けられたデータを基にして、第２の鍵を生成するように構成してもよい。

【００３７】この構成によると、特定のタイトルデータの鍵データが不正に入手されたとしても、その鍵データを用いて他のタイトルデータの復号ができず、他のタイトルデータに対する不正なアクセスからは保護されるという効果がある。また、本発明は、媒体を識別する識別子と、データを暗号化する第２の鍵を前記識別子を基にして生成された第１の鍵を用いて暗号化した暗号化鍵と、前記第２の鍵を用いて暗号化された暗号化データとをあらかじめ記録しているデジタル記録媒体よりデータを読み出して、復号化するデータ復号化装置であって、前記デジタル記録媒体より前記識別子を読み出し、読み出した識別子を基にして第１の鍵を生成する第１の鍵生成手段と、前記デジタル記録媒体より前記暗号化鍵と前記暗号化データとを読み出す読出手段と、前記読み出された暗号化鍵を、前記生成された第１の鍵を基にして復号化し、第２の鍵を生成する鍵復号化手段と、前記生成された第２の鍵を用いて、前記読み出された暗号化データを復号化するデータ復号化手段とを備える。

【００３８】この構成によると、デジタル記録媒体毎に異なり固有に割り付けられた識別子から生成した鍵を用いて、暗号化された鍵データ自身を復号化するので、媒体全体が不正に複製された場合に、タイトルデータを正しく復号できず、その結果、タイトルデータに対する不正なアクセスから保護されるという効果がある。また、暗号化されたタイトルデータは、タイトルデータ毎に異なった鍵データによって復号化が行なわれる為、あるタイトルデータの暗号化に使用された鍵データが不正に入手されても、デジタル記録媒体上の他のタイトルデータに対する不正なアクセスからは保護されるという効果があり、その結果としてデジタル記録媒体の不正な複製や、タイトルデータの鍵データ不正入手に対しても高いセキュリティの実現が可能となる。

【００３９】ここで、前記データ復号化手段は、前記生成された第２の鍵を用いて、前記読み出された暗号化データを復号化する副復号化手段と、前記復号化されたデータが所定の形式を形成しているかどうかを判断する形式判断手段と、前記形式判断手段により所定の形式を形成していると判断された場合には、復号化されたデータを出力し、所定の形式を形成していないと判断された場合には、復号化されたデータの出力を抑制するデータ出力手段とを備えるように構成してもよい。

【００４０】この構成によると、再生しようとする媒体又はタイトルデータが不正に複製されたものである場合に、正しくない鍵データを用いて復号すると、誤った内容のタイトルデータが復号され、ＭＰＥＧなど規格に合致しないことが分かるので、直ちに当該復号処理を中止することができる。その結果、意味のない復号処理を省略して復号処理時間を短縮できるという効果がある。

【００４１】また、本発明は、媒体を識別する識別子と、データを暗号化する第２の鍵を前記識別子を基にし

て生成された第１の鍵を用いて暗号化した暗号化鍵と、前記第２の鍵を用いて暗号化された暗号化データとをあらかじめ記録しているデジタル記録媒体にデータを暗号化して記録し、記録されたデータを読み出して、復号化するデータ暗号化復号化装置であって、データの入力を受け付ける入力受付手段と、前記デジタル記録媒体より前記識別子を読み出し、読み出した識別子を基にして第１の鍵を生成する第１の鍵生成手段と、前記入力を受け付けられたデータ毎に第２の鍵を生成する第２の鍵生成手段と、前記入力を受け付けられたデータを前記第２の鍵を用いて暗号化し、暗号化データを生成するデータ暗号化手段と、前記第２の鍵を前記第１の鍵を用いて暗号化し、暗号化鍵を生成する鍵暗号化手段と、前記生成された暗号化データと前記生成された暗号化鍵とを前記デジタル記録媒体に記録する記録手段と、前記デジタル記録媒体より前記暗号化鍵と前記暗号化データとを読み出す読出手段と、前記読み出された暗号化鍵を、前記生成された第１の鍵を基にして復号化し、第２の鍵を生成する鍵復号化手段と、前記生成された第２の鍵を用いて、前記読み出された暗号化データを復号化するデータ復号化手段とを備える。

【００４２】この構成によると、デジタル記録媒体毎に異なり固有に割り付けられた識別子から生成した鍵を用いて、タイトルデータを暗号化したその鍵データ自身を暗号化するので、暗号化タイトルデータを復号する際の鍵データ自身の保護強度を高めるという効果がある。また、タイトルデータ毎に異なった鍵データによって暗号化が行なわれる為、あるタイトルデータの暗号化に使用された鍵データが不正に入手されても、デジタル記録媒体上の他のタイトルデータに対する不正なアクセスからは保護されるという効果があり、その結果としてデジタル記録媒体の不正な複製や、タイトルデータの鍵データ不正入手に対しても高いセキュリティの実現が可能となる。

【００４３】また、デジタル記録媒体毎に異なり固有に割り付けられた識別子から生成した鍵を用いて、暗号化された鍵データ自身を復号化するので、媒体全体が不正に複製された場合に、タイトルデータを正しく復号できず、その結果、タイトルデータに対する不正なアクセスから保護されるという効果がある。また、暗号化されたタイトルデータは、タイトルデータ毎に異なった鍵データによって復号化が行なわれる為、あるタイトルデータの暗号化に使用された鍵データが不正に入手されても、デジタル記録媒体上の他のタイトルデータに対する不正なアクセスからは保護されるという効果があり、その結果としてデジタル記録媒体の不正な複製や、タイトルデータの鍵データ不正入手に対しても高いセキュリティの実現が可能となる。

【００４４】ここで、前記第２の鍵生成手段は、乱数を発生させ、発生された乱数を基にして第２の鍵を生成するように構成してもよい。この構成によると、鍵データが乱数を基に生成されるので、鍵データを発見されにくくするという効果がある。ここで、前記第２の鍵生成手段は、前記入力を受け付けられたデータを基にして、第２の鍵を生成するように構成してもよい。

【００４５】この構成によると、特定のタイトルデータの鍵データが不正に入手されたとしても、その鍵データを用いて他のタイトルデータの復号ができず、他のタイトルデータに対する不正なアクセスからは保護されるという効果がある。ここで、前記データ復号化手段は、前記生成された第２の鍵を用いて、前記読み出された暗号化データを復号化する副復号化手段と、前記復号化されたデータが所定の形式を形成しているかどうかを判断する形式判断手段と、前記形式判断手段により所定の形式を形成していると判断された場合には、復号化されたデータを出力し、所定の形式を形成していないと判断された場合には、復号化されたデータの出力を抑制するデータ出力手段とを備えるように構成してもよい。

【００４６】この構成によると、再生しようとする媒体又はタイトルデータが不正に複製されたものである場合に、正しくない鍵データを用いて復号すると、誤った内容のタイトルデータが復号され、ＭＰＥＧなど規格に合致しないことが分かるので、直ちに当該復号処理を中止することができる。その結果、意味のない復号処理を省略して復号処理時間を短縮できるという効果がある。

【００４７】また、本発明は、媒体を識別する識別子をあらかじめ記録しているデジタル記録媒体にデータを暗号化して記録するデータ暗号化方法であって、データの入力を受け付ける入力受付ステップと、前記デジタル記録媒体より前記識別子を読み出し、読み出した識別子を基にして第１の鍵を生成する第１の鍵生成ステップと、前記入力を受け付けられたデータ毎に第２の鍵を生成する第２の鍵生成ステップと、前記入力を受け付けられたデータを前記第２の鍵を用いて暗号化し、暗号化データを生成するデータ暗号化ステップと、前記第２の鍵を前記第１の鍵を用いて暗号化し、暗号化鍵を生成する鍵暗号化ステップとを含み、前記生成された暗号化データと前記生成された暗号化鍵とを前記デジタル記録媒体に記録する。

【００４８】この方法を用いると、デジタル記録媒体毎に異なり固有に割り付けられた識別子から生成した鍵を用いて、タイトルデータを暗号化したその鍵データ自身を暗号化するので、暗号化タイトルデータを復号する際の鍵データ自身の保護強度を高めるという効果がある。また、タイトルデータ毎に異なった鍵データによって暗号化が行なわれる為、あるタイトルデータの暗号化に使用された鍵データが不正に入手されても、デジタル記録媒体上の他のタイトルデータに対する不正なアクセスからは保護されるという効果があり、その結果としてデジタル記録媒体の不正な複製や、タイトルデータの鍵デー

タ不正入手に対しても高いセキュリティの実現が可能となる。

【００４９】ここで、前記第２の鍵生成ステップは、乱数を発生させ、発生された乱数を基にして第２の鍵を生成するように構成してもよい。この方法を用いると、鍵データが乱数を基に生成されるので、鍵データを発見されにくくするという効果がある。ここで、前記第２の鍵生成ステップは、前記入力を受け付けられたデータを基にして、第２の鍵を生成するように構成してもよい。

【００５０】この方法を用いると、特定のタイトルデータの鍵データが不正に入手されたとしても、その鍵データを用いて他のタイトルデータの復号ができず、他のタイトルデータに対する不正なアクセスからは保護されるという効果がある。また、本発明は、媒体を識別する識別子と、データを暗号化する第２の鍵を前記識別子を基にして生成された第１の鍵を用いて暗号化した暗号化鍵と、前記第２の鍵を用いて暗号化された暗号化データとをあらかじめ記録しているデジタル記録媒体よりデータを読み出して、復号化するデータ復号化方法であって、前記デジタル記録媒体より前記識別子を読み出し、読み出した識別子を基にして第１の鍵を生成する第１の鍵生成ステップと、前記デジタル記録媒体より前記暗号化鍵と前記暗号化データとを読み出す読出ステップと、前記読み出された暗号化鍵を、前記生成された第１の鍵を基にして復号化し、第２の鍵を生成する鍵復号化ステップと、前記生成された第２の鍵を用いて、前記読み出された暗号化データを復号化するデータ復号化ステップとを含む。

【００５１】この方法を用いると、デジタル記録媒体毎に異なり固有に割り付けられた識別子から生成した鍵を用いて、暗号化された鍵データ自身を復号化するので、媒体全体が不正に複製された場合に、タイトルデータを正しく復号できず、その結果、タイトルデータに対する不正なアクセスから保護されるという効果がある。また、暗号化されたタイトルデータは、タイトルデータ毎に異なった鍵データによって復号化が行なわれる為、あるタイトルデータの暗号化に使用された鍵データが不正に入手されても、デジタル記録媒体上の他のタイトルデータに対する不正なアクセスからは保護されるという効果があり、その結果としてデジタル記録媒体の不正な複製や、タイトルデータの鍵データ不正入手に対しても高いセキュリティの実現が可能となる。

【００５２】ここで、前記データ復号化ステップは、前記生成された第２の鍵を用いて、前記読み出された暗号化データを復号化する副復号化ステップと、前記復号化されたデータが所定の形式を形成しているかどうかを判断する形式判断ステップと、前記形式判断ステップにより所定の形式を形成していると判断された場合には、復号化されたデータを出力し、所定の形式を形成していないと判断された場合には、復号化されたデータの出力を抑制するデータ出力ステップとを備えるように構成してもよい。

【００５３】この方法を用いると、再生しようとする媒体又はタイトルデータが不正に複製されたものである場合に、正しくない鍵データを用いて復号すると、誤った内容のタイトルデータが復号され、ＭＰＥＧなど規格に合致しないことが分かるので、直ちに当該復号処理を中止することができる。その結果、意味のない復号処理を省略して復号処理時間を短縮できるという効果がある。

【００５４】また、本発明は、以上に説明したデータ暗号化プログラム及びデータ復号化プログラムを記録したコンピュータ読み取り可能な記録媒体であるので、上記データ暗号化方法及びデータ復号化方法をコンピュータに実行させることにより、上記データ暗号化装置、データ復号化装置、データ暗号化復号化装置と同様の効果を奏することは明らかである。

【００５５】また、本発明は、媒体を識別する識別子と、データを暗号化する第２の鍵を前記識別子を基にして生成された第１の鍵を用いて暗号化した暗号化鍵と、前記第２の鍵を用いて暗号化された暗号化データとをあらかじめ記録しているデジタル記録媒体である。この媒体を用いると、デジタル記録媒体毎に異なり固有に割り付けられた識別子から生成した鍵を用いて、タイトルデータを暗号化したその鍵データ自身が暗号化されているので、暗号化タイトルデータを復号する際の鍵データ自身の保護強度を高めるという効果がある。

【図面の簡単な説明】

【図１】本発明に係る一つの実施形態としてのデータ暗号化復号化装置のブロック構成図である。

【図２】図１に示すデータ暗号化復号化装置のデータ記録動作を示すフローチャートである。

【図３】図１に示すデータ暗号化復号化装置のデータ再生動作を示すフローチャートである。

【図４】従来のデータ複製管理装置としてのＤＡＴカセットシステムのブロック構成図である。

【図５】従来の光ディスクの不正コピー防止装置の記録部の構成図である。

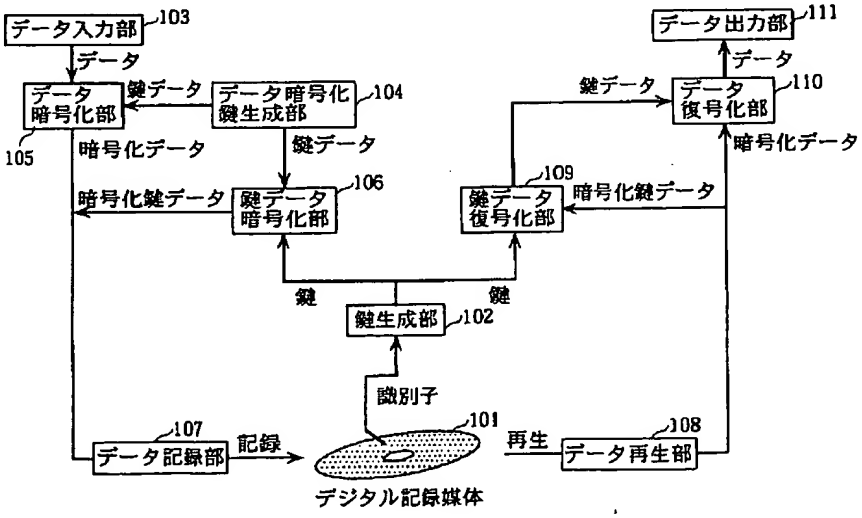
【図６】従来の光ディスクの不正コピー防止装置の再生部の構成図である。

【符号の説明】

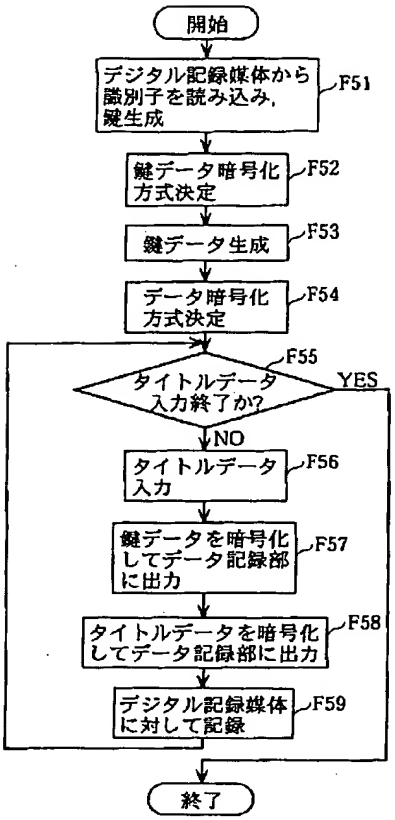
１０１・・・デジタル記録媒体
１０２・・・鍵生成部
１０３・・・データ入力部
１０４・・・データ暗号化鍵生成部
１０５・・・データ暗号化部
１０６・・・鍵データ暗号化部
１０７・・・データ記録部
１０８・・・データ再生部
１０９・・・鍵データ復号化部
１１０・・・データ復号化部

１１１・・・データ出力部
２１・・・データ入力部
２２・・・制御情報管理部
２３・・・デジタル記録媒体
２４・・・データ出力部
３１・・・光ディスクのキー情報記録領域
３２・・・光ディスクのデータ記録領域
３３・・・原データに対する暗号化手段
３４・・・光ディスクに対して主データを記録する主データ記録手段
３５・・・光ディスクに対してキー情報を記録するキー情報記録手段
４１・・・光ディスクのキー情報記録領域
４２・・・光ディスクのデータ記録領域
４３・・・光ディスクから主データを読み込む主データ読取手段
４４・・・光ディスクからキー情報を読み込むキー情報読取手段
４５・・・主データに対する復号化手段
Ｆ５１・・・デジタル記録媒体から読み込んだ識別子を元に鍵を生成するステップ
Ｆ５２・・・生成した鍵により暗号化方法を決定するステップ
Ｆ５３・・・タイトルデータに対するタイトルコードまたは発生した乱数を元に鍵データを生成するステップ
Ｆ５４・・・生成した鍵データにより暗号化方法を決定するステップ
Ｆ５５・・・タイトルデータの入力終了を判断するステップ
Ｆ５６・・・タイトルデータを入力するステップ
Ｆ５７・・・鍵データを暗号化するステップ
Ｆ５８・・・タイトルデータを鍵データを元に暗号化するステップ
Ｆ５９・・・暗号化された鍵データとタイトルデータをデジタル記録媒体に記録するステップ
Ｆ６１・・・デジタル記録媒体から読み込んだ識別子を元に鍵を生成するステップ
Ｆ６２・・・生成した鍵により復号化方式を決定するステップ
Ｆ６３・・・デジタル記録媒体から暗号化された鍵データを読み込むステップ
Ｆ６４・・・鍵データを復号化するステップ
Ｆ６５・・・復号化した鍵データによる復号化方法を決定するステップ
Ｆ６６・・・デジタル記録媒体から暗号化されたタイトルデータを読み込むステップ
Ｆ６７・・・タイトルデータの読込み終了を判断するステップ
Ｆ６８・・・暗号化されたタイトルデータを鍵データを元に復号化するステップ
Ｆ６９・・・復号化されたタイトルデータを出力するステップ

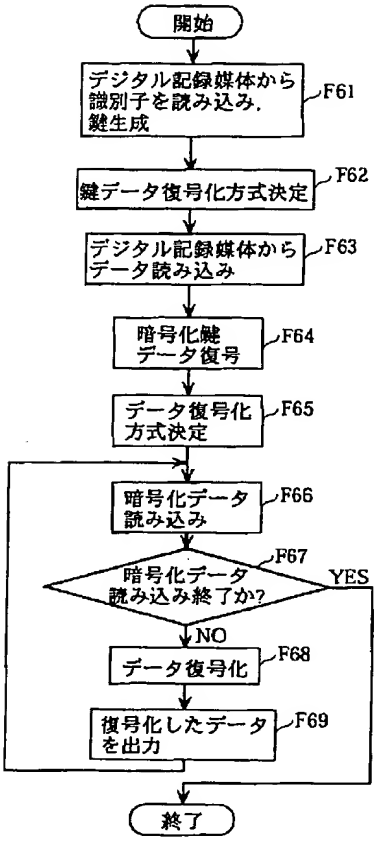
【図１】



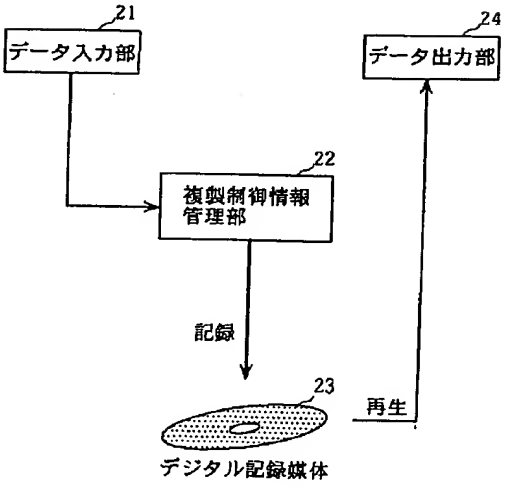
【図2】


開始
デジタル記録媒体から識別子を読み込み，鍵生成
F51
鍵データ暗号化方式決定
F52
鍵データ生成
F53
データ暗号化方式決定
F54
タイトルデータ入力終了か?
F55
YES
NO
タイトルデータ入力
F56
鍵データを暗号化してデータ記録部に出力
F57
タイトルデータを暗号化してデータ記録部に出力
F58
デジタル記録媒体に対して記録
F59
終了

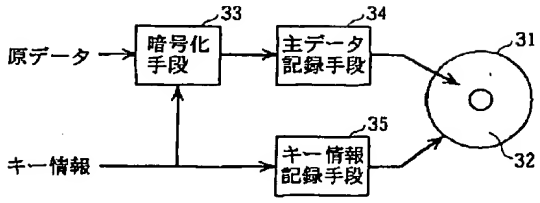
【図3】


開始
デジタル記録媒体から識別子を読み込み，鍵生成
F61
鍵データ復号化方式決定
F62
デジタル記録媒体からデータ読み込み
F63
暗号化鍵データ復号
F64
データ復号化方式決定
F65
暗号化データ読み込み
F66
暗号化データ読み込み終了か?
F67
YES
NO
データ復号化
F68
復号化したデータを出力
F69
終了

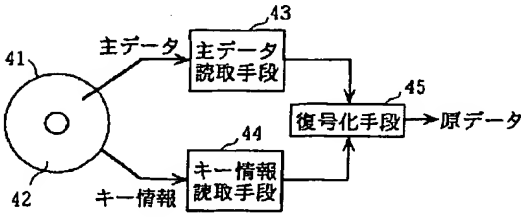
【図4】


21
データ入力部
22
複製制御情報管理部
記録
23
デジタル記録媒体
再生
24
データ出力部

【図5】


原データ
33
暗号化手段
34
主データ記録手段
31
キー情報
35
キー情報記録手段
32

【図6】


41
主データ
43
主データ読取手段
45
復号化手段
原データ
44
キー情報読取手段
42
キー情報